

**TO: Clerk's Office
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK**



**APPLICATION FOR LEAVE
TO FILE DOCUMENT UNDER SEAL**

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR A SEARCH WARRANT FOR A
DISCOU JNT AS DESCRIBED
FURTHER CHMENT A

20-MJ-423

Docket Number

SUBMITTED BY: Plaintiff ___ Defendant ___ DOJ ☒

Name: AUSA Josh Hafetz

Firm Name: USAO-EDNY

Address: _____

Phone Number: 929-888-4077

E-Mail Address: joshua.hafetz@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES ___ NO ☒

If yes, state description of document to be entered on docket sheet:

MANDATORY CERTIFICATION OF SERVICE:

A.) ___ A copy of this application either has been or will be promptly served upon all parties to this action, B.) ___ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation: _____; or C.) ☒ This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

June 8, 2020

DATE

SIGNATURE

A) If pursuant to a prior Court Order:

Docket Number of Case in Which Entered: _____

Judge/Magistrate Judge: _____

Date Entered: _____

B) If a new application, the statute, regulation, or other legal basis that authorizes filing under seal

Ongoing investigation; see SW Affidavit

**ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE,
AND MAY NOT BE UNSEALED UNLESS ORDERED BY
THE COURT.**

DATED: Brooklyn, NEW YORK

Josh Hafetz

June 9, 2020

U.S. MAGISTRATE JUDGE

RECEIVED IN CLERK'S OFFICE _____

DATE

RMT:JAM/JGH
F.# 2020R00515

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR A SEARCH WARRANT FOR THE
FOLLOWING DISCORD, INC. ACCOUNT
BEARING USER ID 280192627549274112
AS FURTHER DESCRIBED IN
ATTACHMENT A

TO BE FILED UNDER SEAL

**APPLICATION FOR A
SEARCH WARRANT**

No. 20-MJ- 423

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, COLIN J. MCLAFFERTY, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant to search for information that is stored at premises controlled by Discord, Inc. (“Discord” or the “Provider”), a provider of electronic communication and remote computing services, headquartered at 444 De Haro Street, Suite 200, San Francisco, California 94107, associated with the following account identified bearing the User ID 280192627549274112 and the User Name dzenan#6672 (the “TARGET ACCOUNT”).¹

¹ Because this Court has jurisdiction over the offense(s) being investigated, it may issue the warrant to compel the provider pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) (“A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction”) and 2711 (“the term ‘court of

2. The information to be searched is described in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(d) to require the Provider to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B.

3. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) currently assigned to the New York Joint Terrorism Task Force (“JTTF”). I have participated in numerous investigations, during the course of which I have conducted physical surveillance, interviewed witnesses, executed court-authorized search warrants and used other techniques to secure relevant information.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses, including confidential sources. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Where the contents of documents and written communications are summarized

competent jurisdiction’ includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title”).

herein, they are done so in sum and substance and in pertinent part unless otherwise indicated.

BACKGROUND ON ISIS

5. On or about October 15, 2004, the United States Secretary of State designated al-Qaeda in Iraq (“AQI”), then known as Jam’at al Tawhid wa’ al-Jihad, as a Foreign Terrorist Organization (“FTO”) under Section 219 of the Immigration and Nationality Act, and as a Specially Designated Global Terrorist entity under Section 1(b) of Executive Order 13224. On or about December 11, 2012, the Secretary of State amended the designation of AQI to include the following aliases: al-Nusrah Front (“ANF”), Jabhat al-Nusrah, Jabhet al-Nusra, The Victory Front, and Al-Nusrah Front for the People of the Levant.

6. On or about May 15, 2014, the Secretary of State, in response to the evolving nature of the relationships between ANF and AQI, amended the designation of AQI as an FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224, to add the alias Islamic State of Iraq and the Levant (“ISIL”) as its primary name and to remove all aliases associated with al-Nusrah Front. The Secretary of State also added the following aliases to the FTO listing: The Islamic State of Iraq and al-Sham (ISIS - which is how the FTO will be referenced herein), The Islamic State of Iraq and Syria, ad-Dawla al-Islamiyya fi al-Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. On September 21, 2015, the Secretary added the following aliases to the ISIS FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

7. Based on my training and experience, my personal participation in this and other investigations involving ISIS, my conversations with other law enforcement agents who have been involved in ISIS-related investigations, and my review of publically available materials, I have learned that to gain supporters, ISIS, like many other terrorist organizations, spreads its message using social media, Internet platforms, and sites on the “dark web.”² Using these platforms, ISIS posts and circulates videos and updates of events in Syria, Iraq, and areas with an ISIS presence, in English and Arabic, as well as other languages, to draw support to its cause.

8. Most recently, based on publically available materials, I have learned that ISIS supporters have taken an interest in the rioting, looting and other violence attendant to the series of largely-peaceful demonstrations and protests throughout the United States in or about late May 2020 and early June 2020, and has directed ISIS supporters to commit acts of violence in the United States during this period of time. Specifically, pro-ISIS social media accounts have featured police cars burning and other violent imagery. For example, on “Shamukh,” which is an ISIS-related forum on the dark web, a series of threads on or about May 31, 2020 urged supporters in the United States to exploit current social tensions by carrying out physical attacks against law enforcement and protesters to sow further discord.

² The dark web is content that exists on the Internet but is not indexed by traditional search engines. Dark web content requires specific software or applications to access, such as TOR, or “The Onion Router,” which was used by CAMOVIC and described below.

THE INVESTIGATION

9. The JTTF is investigating DZENAN CAMOVIC and others for an attack on multiple New York City Police Department (“NYPD”) officers on or about June 3, 2020. The investigation involves violations of, among other statutes, 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder), 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien); 18 U.S.C. § 924(c) (use of a firearm during a crime of violence); 18 U.S.C. § 1951 (Hobbs Act Robbery); and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization (“FTO”) (collectively the “Subject Offenses”).

10. On or about June 3, 2020, at approximately 11:50 p.m., CAMOVIC approached two uniformed NYPD officers in the vicinity of 885 Flatbush Avenue in Brooklyn, New York. The two officers were assigned to an anti-looting post that evening, including the responsibility for enforcing the curfew. Security camera footage from the area shows CAMOVIC walking on Flatbush Avenue toward the intersection of Flatbush and Church Avenues. Upon reaching the corner of Flatbush and Church Avenues, CAMOVIC turned onto Church Avenue, where the two NYPD officers stood on patrol. The surveillance video shows that, upon turning the corner in the direction of the police officers, CAMOVIC immediately stabbed one of the officers in the neck area with a knife he already had in his hand, and then began chasing the second officer, repeatedly and violently stabbing at the officer in a clear attempt to kill him. CAMOVIC then ran back toward the first officer, whom he had already stabbed, and attempted to stab him again.

11. A struggle ensued. Video footage from the officer's body camera shows that CAMOVIC fought for control of the officer's service weapon. CAMOVIC ultimately gained control of the weapon, thereby robbing the officer of his service weapon through the use of force.

12. CAMOVIC can also be heard on body camera video repeatedly yelling "Allahu Akbar" during the attack. Based on my knowledge, training and experience, I know that "Allahu Akbar" is an Arabic phrase that means "God is the greatest" and has been shouted by perpetrators of violent jihadist attacks during such attacks.

13. After gaining control of the officer's service weapon, CAMOVIC fired multiple shots at several officers, including at one or more officers who responded to the scene. Several officers were wounded as a result of CAMOVIC's attack.

14. CAMOVIC was ultimately shot by responding officers and taken into custody. The officer's service weapon taken and used by CAMOVIC, a SIG Sauer P226 black semiautomatic 9mm handgun, was recovered from the scene.

15. Based on my training and experience, I know that the NYPD has a presence, and employs police officers and other employees that operate in their official capacity, in multiple locations outside of New York State and outside of the United States.

16. Based on my knowledge, training and experience, I know that the officer's service weapon was manufactured outside the state of New York.

17. The investigation has revealed that CAMOVIC is a 20 year-old resident of Brooklyn, New York. He is a Bosnian national who was born in Germany. He has no legal immigration status in the United States.

18. Law enforcement officers searched CAMOVIC's person incident to his arrest immediately after his attack on police on June 3, 2020, during which time they recovered an LG cellular phone ("the CAMOVIC LG Phone"). On June 4, 2020, this Court issued a search warrant authorizing law enforcement agents to search the CAMOVIC LG Phone for evidence of certain of the Subject Offenses.

19. Additionally, pursuant to the investigation, several electronic devices and electronic media were recovered from CAMOVIC's residence at 580 East 22nd Street, Apartment #5 Brooklyn New, York 11226, pursuant to a consensual search. On June 5 and June 6, 2020, the Honorable Steven M. Gold, Magistrate Judge for the Eastern District of New York, granted two search warrants to search those items. On June 7, 2020, Judge Gold issued an additional search warrant related to the search of the CAMOVIC LG Phone and the multiple electronic devices found in CAMOVIC's room following his June 3, 2020 attack on police.

20. Phone records and other evidence show that, inter alia, CAMOVIC used the CAMOVIC LG Phone to exchange multiple text messages with several individuals in the hours before his attack on the police officers.

21. A review of the CAMOVIC LG Phone has revealed further that CAMOVIC downloaded and used an application called Orbot. Orbot is a mobile application used for the Tor network. Tor, in turn, is a computer network designed to facilitate anonymous communication over the Internet. The Tor network accomplishes this by routing a user's communications through a globally distributed network of relay computers, or proxies, rendering ineffective any conventional Internet Protocol ("IP") address-based methods of

identifying users. To access the Tor network, a user installs specific Tor software. The Tor network also enables users to operate hidden sites that operate similarly to conventional websites. The Tor network permits a user to conduct internet activity with a high degree of privacy and anonymity. As a result, the network is often used by individuals involved in criminal activity that want to obscure their identity and evade law enforcement.

22. Here, it appears that CAMOVIC downloaded and began using Orbot to connect to the Tor network on or about June 1, 2020—two days prior to his attack. CAMOVIC appears to have connected and used the application on several occasions thereafter. On or about June 2, 2020 at approximately 10:00 p.m. New York time – less than 24 hours before the attack – CAMOVIC deleted the application. It appears that CAMOVIC may have been attempting to delete evidence of his criminal activity.

23. Additionally, the review of the CAMOVIC LG Phone also indicates that CAMOVIC downloaded and used a mobile application called Citizen shortly before the attack. Citizen is a social media application that allows users to send and receive information about local events associated with law enforcement activity. According to its website, Citizen describes itself as a “safety app that give you instant access to verified 911 information.”

24. A user of the Citizen application located in or around the New York City region would receive alerts and information pertaining to NYPD law enforcement activity. In particular, during the relevant time period, a user of the Citizen application would have received information about NYPD activity related to the ongoing protests, looting and civil disorder. The application also allows users to submit and upload information and videos

pertaining to such activity. The application provides mapping and location information for these events, and so a user would be able to learn about locations where NYPD are present.

25. CAMOVIC downloaded the Citizen application on or about June 2, 2020 and accessed the application on several occasions prior to his attack, including on June 3, 2020, shortly before the attack on law enforcement.

26. Additionally, according to records provided by the company that operates Citizen, CAMOVIC's service began on or about May 26, 2018, which indicates that CAMOVIC utilized Citizen on one or more previous mobile devices, such as the cellular phones found at his residence.

27. Based on the above, it appears that CAMOVIC was researching law enforcement-related activity shortly before he attacked the NYPD officers. Furthermore, based on my training and experience, I know that individuals associated with or supporting foreign terrorist organizations and involved in terrorist attacks will sometimes use technology like the Tor network to obtain information and communicate with one another.

28. Law enforcement's review of the electronic devices recovered from CAMOVIC's bedroom has further revealed that CAMOVIC was in possession of materials reflecting support for designated foreign terrorist organizations such as ISIS and demonstrating CAMOVIC's interest in jihadist materials.

29. For example, the review of the contents of a Sandisk 64 GB hard drive seized from CAMOVIC's bedroom—which itself contained no label or date on the physical body of the items—revealed over 175 file folders and 15 images. According to data on the hard drive, each of these files reflected creation dates of March 29, 2019, and the majority of the

files were last accessed on October 21, 2019. Specifically, the file names on the Sandisk 64 GB hard drive appear related to extremist Salafi Islam religious content, including notable figures associated with designated foreign terrorist organizations. The files include hundreds of audio files that, according to their file names and based on my knowledge, training and experience, are files of speeches by Anwar al-Awlaki and media products released by ISIS. For example, one file is titled “The Dust Will Never Settle Down.” In a speech of that name, al-Awlaki advocated violence against individuals that he believed defamed and mocked Islam. Another file, titled “Constants on the Path of Jihad” is the same title of another speech by al-Awlaki where he argued that the concept of “jihad” denoted combat against disbelievers rather than an internal struggle.

30. The Sandisk 64 GB hard drive also contains a file with the Arabic text, “Saleel al Sawarim,” which I understand translates roughly into English as “The Clanging of Swords.” I know that a song of that name was a popular Arabic song attributed to ISIS.

31. Additionally, 21 CDs seized by law enforcement during the search of CAMOVIC’s bedroom at his residence bear labels with descriptions such as “Young Aisha – Imam Anwar al A’wlaqi,” and “Lives of the Prophets,” a lecture series of Awlaki, reflecting that the contents of such files likely contain evidence of radical Islamic beliefs.

THE TARGET ACCOUNT

32. On or about June 8, 2020, law enforcement individuals interviewed an associate of CAMOVIC (“Individual 4”).³ Individual 4 informed law enforcement that

³ The prior search warrant affidavits in this case refer to other associates of CAMOVIC as “Individuals 1, 2, and 3.”

he/she and CAMOVIC have been friends since childhood. Individual 4 informed law enforcement that recently, in addition to spending time and playing video games with CAMOVIC, the two also communicated over the communications platform Discord.

33. Discord is an application and digital distribution platform designed for creating communities comprising many different types of people, ranging from gamers to educators and business executives. Discord specializes in text, image, video and audio communication between users in a chat channel and allows users to send direct messages to each other. Discord has both a desktop application and a mobile application, and the service can also be accessed from a website.

34. Both CAMOVIC and Individual 4 are Muslim, and Individual 4 informed law enforcement that beginning approximately six months ago, he/she noticed that CAMOVIC was becoming more religiously observant. Individual 4 believed CAMOVIC's becoming more religious was a positive development because, prior to that, CAMOVIC had a violent temper and often started physical altercations over perceived slights and, as he became more religious, CAMOVIC's angry outbursts began to dissipate. However, Individual 4 also informed law enforcement that around the time of Ramadan in approximately April 2020, CAMOVIC used the TARGET ACCOUNT to send Individual 4 two videos of a sermon by an imam. Individual 4 informed law enforcement that he/she did not open the videos CAMOVIC sent via Discord because he/she feared that the content of the videos might get Individual 4 in trouble. Individual 4 further informed law enforcement that after CAMOVIC sent him/her the two videos on Discord in or around April 2020, CAMOVIC repeatedly asked Individual 4 if he/she had watched the videos.

35. Records for the TARGET ACCOUNT show that it was created on or about February 12, 2017 and is registered to CAMOVIC and is associated with CAMOVIC's email address dzenancamovic123@gmail.com. Records for the TARGET ACCOUNT further show that CAMOVIC used the account numerous times in the days and weeks leading up to his June 3, 2020 attack on NYPD officers. Indeed, the records show that the TARGET ACCOUNT was accessed at approximately 10:03 p.m. and 11:06 p.m. on June 3, 2020, less than an hour before CAMOVIC attacked the police. Records recovered from the search of the CAMOVIC LG Phone indicate that CAMOVIC had the Discord application installed on the phone, which was on his person at the time of his June 3, 2020 attack on police.

36. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to search the TARGET ACCOUNT, described in Attachment A, for evidence of the Subject Offenses as described in Attachment B.

BACKGROUND ON DISCORD

37. As a general matter, it is my understanding based on my training and experience that providers of online communications and social media services, like Discord, offer a variety of online services to the public. Providers like Discord allow subscribers to obtain accounts like the TARGET ACCOUNT. Subscribers obtain an account by registering with the provider. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for the account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and for paying subscribers, means and source of payment (including any credit or bank account number). Some providers also maintain a

record of changes that are made to the information provided in subscriber records, such as to any other e-mail addresses or phone numbers supplied in subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user or users of an account.

38. As noted above, Discord is an online messaging application and digital distribution platform. Among other things, a user of Discord can create and join “servers,” and participate in “channels” within each server, where the user can communicate and interact with other users of Discord. There are both text channels (where a user can communicate by text and also send and receive, photos, videos and other types of files) and voice channels (where users can communicate by audio communications). Users can also communicate through direct messages, which are private chats created between 1-10 users

39. Based on the Discord Privacy Policy, which is available online, I know the following about the collection and preservation of data at Discord:

40. Discord collects information from users when they voluntarily provide such information, such as when they register for access to the Discord application and related Internet services (the “Services”). Information Discord collects may include but not be limited to username, email address, and any messages, images, transient voice-over-internet-protocol (“VOIP”) data (to enable communication delivery only) or other content users send via the chat feature.

41. When users interact with Discord through the Services, Discord receives and stores certain information such as an IP address, device ID, and the user’s activities within the Services. Discord may store such information or such information may be included in

databases owned and maintained by affiliates, agents or service providers. The Services may use such information and pool it with other information to track, for example, the total number of visitors to Discord's website, the number of messages users have sent, and the domain names of visitors' Internet service providers.

42. Users may give Discord permission to collect their information in other services. For example, a user may connect a social networking service ("SNS") such as Facebook or Twitter to their Discord account. When a user does this, it allows Discord to obtain information from those accounts (for example, a user's friends or contacts).

43. Discord employs cookies and similar technologies to keep track of users' local computer's settings such as which account users have logged into and notification settings. Cookies are pieces of data that sites and services can set on a user's browser or device that can be read on future visits. Discord may expand its use of cookies to save additional data as new features are added to the Service. In addition, Discord uses technologies such as web beacons and single-pixel gifs to record log data such as open rates for emails sent by the system.

44. Discord may use third party web site analytic tools such as Google Analytics on its website that employ cookies to collect certain information concerning use of its Services. However, users can disable cookies by changing their browser settings.

45. Accordingly, based on the above, the computers of the Provider are likely to contain stored electronic communications and information concerning subscribers and their use of the Provider's services, such as account access information, communications and message transaction information, and account application information. In my training and

experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the TARGET ACCOUNT.

46. A subscriber of the Provider can also store with the Provider files in addition to text-based messages, such as image and video files, on servers maintained and/or owned by the Provider. In my training and experience, evidence of who was using an account may be found in such information.

47. In my training and experience, providers like Discord typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, providers like Discord often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the TARGET ACCOUNT.

48. In my training and experience, users of online services like Discord will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of e-mails and social media services typically retain records about such communications, including records of contacts between the user and the provider's support

services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the TARGET ACCOUNT.

49. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account, including the e-mail addresses or account identifiers and messages sent to that account, often provides important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of the TARGET ACCOUNT, I am requesting a warrant requiring the Provider to turn over all information associated with the

TARGET ACCOUNT with the date restriction included in Attachment B for review by the search team.

50. Relatedly, the government must be allowed to determine whether other individuals had access to the TARGET ACCOUNT. If the government were constrained to review only a subsection of an account, that subsection might give the misleading impression that only a single user had access to the account.

51. In my training and experience, providers typically keep a record of search queries run by the user of an account, whether searches within the services of the provider for persons, content, or other accounts (such as if a user is trying to find the account of an acquaintance), or broader Internet searches. In some instances, providers may also keep records of which websites or contents were “clicked on” as a result of these searches. This information is helpful both in the context of the case to show the topics about which the user was trying to obtain more information or conduct research, and is relevant for “user attribution” evidence, analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

52. I know based on my training and experience that providers of social media services will often keep track of what is referred to as user agent string, which contains information about the type of computer, operating system, and web browser used to access the service. User agent string can include: web requests or HTTP requests (hypertext transfer protocol is the protocol by which many web pages are transmitted between servers and clients or users); logs containing information such as the requestor’s IP address, identity and user ID, date and timestamp, request URL or URI (Uniform Resource Locator or

Indicator, i.e., a website address), HTTP protocol version, referrer, and similar information; login tracker logs; account management logs; and any other e-mail or social media accounts accessed by or analytics related to a Target Account. These can be used to determine the types of devices used while accessing a Target Account, as well as data related to the user's activity while accessing a Target Account.

53. Providers also frequently obtain information about the types of devices that are used to access accounts like the TARGET ACCOUNT. Those devices can be laptop or desktop computers, cellular phones, tablet computers, or other devices. Individual computers or devices are identified by a number of different means, some of which are assigned to a particular device by a manufacturer and connected to the "hardware" or the physical device, some are assigned by a cellular telephone carrier to a particular account using cellular data or voice services, and some are actually assigned by the provider to keep track of the devices using its services. Those device identifiers include Android IDs, Advertising IDs, unique application numbers, hardware models, operating system versions, unique device identifiers, Global Unique Identifiers or "GUIDs," serial numbers, mobile network information, phone numbers, device serial numbers, Media Access Control ("MAC") addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"). Apple, one of the primary suppliers of mobile devices used to access accounts like the TARGET ACCOUNT, had previously used an identifier that was unique to

the hardware of its devices, such that details of a device's activity obtained from a particular application or "app" could be used to target advertisements for the user of that device. Apple replaced that hardware-based identifier with the Apple advertiser ID or IDFA that is still unique to a particular device, but which can be wiped and re-generated anew by a user if a user chooses to do so. Most users, however, do not know that the IDFA exists, and therefore are unaware that their device's activity can be correlated across different apps or services.

54. These device identifiers can then be used (a) to identify accounts accessed at other providers by that same device, and (b) to determine whether any physical devices found in the course of the investigation were the ones used to access each Target Account. The requested warrant therefore asks for the device identifiers, as well as the identity of any other account accessed by a device with the same identifier.

55. Providers of social media services like Discord often maintain, have access to, and store information related to the location of the users of accounts they service. That information may be obtained by the provider in a number of ways. For example, a user may access the provider's services by running an application on the user's phone or mobile device, which application has access to the location information residing on the phone or mobile device, such as Global Positioning System (GPS) information. It may also be accessible through "check-in" features that some providers offer that allow users to transmit or display their location to their "friends" or "acquaintances" via the provider.

56. The subscriber will also generally need to use a password that will allow the user to gain access to the account. Many providers do not store the password directly, rather they use an algorithm (often referred to as a "hashing" algorithm) that is performed on the

password and generates a new random string of numbers and characters, which is what the provider may store. When a user enters his or her password, the hashing algorithm is performed on the password before it is presented to the provider, and the provider will verify the hash value for the password (rather than the password itself) to authorize access to the account. As an added security feature, some providers insert additional text before or after the password, which additional text is referred to as “salting” the password. The hashing algorithm is then performed on the combined password and salt, which is the hash value that will be recognized by the provider. Alternatively or in addition to passwords, users may be required to select or propose a security question, and then provide an answer, which can be used to substitute for a password or to retrieve or reset a user’s password.


57. This application seeks a warrant to search all responsive records and information under the control of the Provider, which is subject to the jurisdiction of this court, regardless of where the Provider has chosen to store such information.

58. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Upon receipt of the search warrant, Discord will then compile the requested records at a time convenient to them, thus reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

REQUEST FOR SEALING

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation that, even though the main target is already in custody, is still in an incipient phase, and it is possible that not all subjects of the investigation are aware of the nature of the government's investigation or the steps that it is taking to collect evidence. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,


Colin J. McLafferty
Special Agent
Federal Bureau of Investigation

SWORN VIA TELEPHONE

Subscribed and sworn to before me on June 9, 2020



THE HONORABLE SANKET J. BULSARA
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information that is stored at premises controlled by Discord, Inc. (“Discord” or the “Provider”), a provider of electronic communication and remote computing services, headquartered at 444 De Haro Street, Suite 200, San Francisco, California 94107, associated with the Discord account bearing the User ID 280192627549274112 and User Name dzenan#6672 (the “Target Account”).

ATTACHMENT B

I. Information to Be Disclosed By the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the Target Account listed in Attachment A:

a. All contents of all wire and electronic communications associated with the Target Account, including:

i. All emails, communications, or messages of any kind associated with the Target Account, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each e-mail or message, and any related documents or attachments;

ii. All records or other information stored by subscriber(s) of the Target Account, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files;

iii. All records pertaining to communications between the Provider and any person regarding the Target Account, including contacts with support services and records of actions taken;

iv. All stored passwords, including passwords stored in clear text and hash form, and for any hashed values that include a salt, the provider shall provide the salt value used to compute the stored password hash value, and any security questions and answers;

v. All search history and web history, including web clicks or “History Events,” by the user of the Target Account; and

vi. All web browsing activities that are identifiable with the Target Account.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other

account names or email addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers, or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, and including any changes made to any subscriber information or services, including specifically changes made to secondary email accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the following account:

(I) The Discord account bearing the User ID 280192627549274112 and User Name dzenan#6672 (the "Target Account");

(II) Any other account associated with the Target Account, including by means of sharing a common secondary, recovery, or alternate email address listed in subscriber records for the Target Account or by means of sharing a common phone number or 5MB number listed in subscriber records for the Target Account, and any account that lists the Target Account as a secondary, recovery, or alternate email address;

(III) Any other account accessed by a device with an identifier responsive to the device identifiers called for below; and

(IV) Any other account associated with the cookie(s) associated with the Target Account.

ii. All user connection logs and transactional information of all activity

relating to the Target Account, described above, including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made;

iii. Any information identifying the device or devices used to access the

Target Account, including any Android 10, Advertising 10, unique application number, hardware model, operating system version, unique device identifier, Global Unique Identifier or "GUID," serial number, mobile network information, phone number, device serial number, MAC address, Electronic Serial Number ("ESN"), Mobile Electronic Identity Number ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Number ("MIN"), Subscriber Identity Module

("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifier ("IMSI"), International Mobile Equipment Identity ("IMEI"), or Apple advertiser ID or ID for advertisers ("IDFA"), or Google's AAID or any other advertiser ID, and any other information regarding the types of devices used to access the Target Account or other device-specific information, including the device type, brand name, device mode or operating system, and first and last times that a device were observed;

iv. Any information showing the location of the user of the Target

Account, including while sending or receiving a message using the

Target Account or accessing or logged into the Target Account; and

v. Any and all cookies used by any computer or web browser associated with the Target Account, including the IP addresses, dates, and times associated with the recognition of any such cookie.

II. Information to be Seized By the Government

For the Target Account listed in Attachment A, all records from the period January 1, 2019 to the present date that relate to violations of federal criminal law by DZENAN CAMOVIC ("CAMOVIC") among others, known and unknown, for the violation of 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder), 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien); 18 U.S.C. § 924(c) (use of a firearm during a crime of violence); 18 U.S.C. § 1951 (Hobbs Act Robbery); and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization (collectively the "Subject Offenses")), including:

- a. Information relating to who created, accessed, or used the Target Account, including records about their identities and whereabouts.
- b. Evidence indicating efforts to provide support to or promote the activities of terrorists and foreign terrorist organizations, including by committing acts of violence in support of such organizations, including ISIS and al-Qaeda in the Arabian Peninsula ("AQAP").
- c. Evidence, including messages, videos, communications, audio recordings, pictures, video recordings, or still captured images relating to jihadist propaganda, including communications regarding support for extremist attacks and support for violent extremist groups, including AQAP and ISIS.
- d. Evidence regarding CAMOVIC's state of mind, including whether and why he harbored any hostile views toward law enforcement and the NYPD.

- e. Evidence of CAMOVIC's close associates, including the individuals with whom he may have had contact in the days leading up to June 3, 2020.
- f. Evidence of CAMOVIC's location at the time he was using the Target Account.
- g. Evidence that may identify any additional coconspirators or aiders and abettors, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the
Eastern District of New York

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)) Case No. 20-MJ-423
IN THE MATTER OF THE APPLICATION OF THE UNITED STATES)
OF AMERICA FOR A SEARCH WARRANT FOR THE FOLLOWING)
DISCORD, INC. ACCOUNT BEARING USER ID 280192627549274112)
AS FURTHER DESCRIBED IN ATTACHMENT A)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before June 22, 2020 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____ the Duty Magistrate Judge
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: Jun 9, 2020 12:08 AM



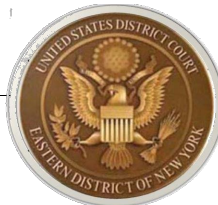
Judge's signature

City and state: Brooklyn, New York

Select Duty Magistrate Judge U.S.M.J.

Printed name and title

SANKET J. BULSARA



AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

ReturnCase No.:
20-

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information that is stored at premises controlled by Discord, Inc. (“Discord” or the “Provider”), a provider of electronic communication and remote computing services, headquartered at 444 De Haro Street, Suite 200, San Francisco, California 94107, associated with the Discord account bearing the User ID 280192627549274112 and User Name dzenan#6672 (the “Target Account”).

.

ATTACHMENT B

I. Information to Be Disclosed By the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the Target Account listed in Attachment A:

a. All contents of all wire and electronic communications associated with the Target Account, including:

i. All emails, communications, or messages of any kind associated with the Target Account, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each e-mail or message, and any related documents or attachments;

ii. All records or other information stored by subscriber(s) of the Target Account, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files;

iii. All records pertaining to communications between the Provider and any person regarding the Target Account, including contacts with support services and records of actions taken;

iv. All stored passwords, including passwords stored in clear text and hash form, and for any hashed values that include a salt, the provider shall provide the salt value used to compute the stored password hash value, and any security questions and answers;

v. All search history and web history, including web clicks or “History Events,” by the user of the Target Account; and

vi. All web browsing activities that are identifiable with the Target Account.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other

account names or email addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers, or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, and including any changes made to any subscriber information or services, including specifically changes made to secondary email accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the following account:

(I) The Discord account bearing the User ID 280192627549274112 and User Name dzenan#6672 (the "Target Account");

(II) Any other account associated with the Target Account, including by means of sharing a common secondary, recovery, or alternate email address listed in subscriber records for the Target Account or by means of sharing a common phone number or 5MB number listed in subscriber records for the Target Account, and any account that lists the Target Account as a secondary, recovery, or alternate email address;

(III) Any other account accessed by a device with an identifier responsive to the device identifiers called for below; and

(IV) Any other account associated with the cookie(s) associated with the Target Account.

ii. All user connection logs and transactional information of all activity

relating to the Target Account, described above, including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made;

iii. Any information identifying the device or devices used to access the

Target Account, including any Android 10, Advertising 10, unique application number, hardware model, operating system version, unique device identifier, Global Unique Identifier or "GUID," serial number, mobile network information, phone number, device serial number, MAC address, Electronic Serial Number ("ESN"), Mobile Electronic Identity Number ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Number ("MIN"), Subscriber Identity Module

("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifier ("IMSI"), International Mobile Equipment Identity ("IMEI"), or Apple advertiser ID or ID for advertisers ("IDFA"), or Google's AAID or any other advertiser ID, and any other information regarding the types of devices used to access the Target Account or other device-specific information, including the device type, brand name, device mode or operating system, and first and last times that a device were observed;

iv. Any information showing the location of the user of the Target

Account, including while sending or receiving a message using the

Target Account or accessing or logged into the Target Account; and

v. Any and all cookies used by any computer or web browser associated with the Target Account, including the IP addresses, dates, and times associated with the recognition of any such cookie.

II. Information to be Seized By the Government

For the Target Account listed in Attachment A, all records from the period January 1, 2019 to the present date that relate to violations of federal criminal law by DZENAN CAMOVIC ("CAMOVIC") among others, known and unknown, for the violation of 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder), 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien); 18 U.S.C. § 924(c) (use of a firearm during a crime of violence); 18 U.S.C. § 1951 (Hobbs Act Robbery); and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization (collectively the "Subject Offenses")), including:

- a. Information relating to who created, accessed, or used the Target Account, including records about their identities and whereabouts.
- b. Evidence indicating efforts to provide support to or promote the activities of terrorists and foreign terrorist organizations, including by committing acts of violence in support of such organizations, including ISIS and al-Qaeda in the Arabian Peninsula ("AQAP").
- c. Evidence, including messages, videos, communications, audio recordings, pictures, video recordings, or still captured images relating to jihadist propaganda, including communications regarding support for extremist attacks and support for violent extremist groups, including AQAP and ISIS.
- d. Evidence regarding CAMOVIC's state of mind, including whether and why he harbored any hostile views toward law enforcement and the NYPD.

- e. Evidence of CAMOVIC's close associates, including the individuals with whom he may have had contact in the days leading up to June 3, 2020.
- f. Evidence of CAMOVIC's location at the time he was using the Target Account.
- g. Evidence that may identify any additional coconspirators or aiders and abettors, including records that help reveal their whereabouts.